ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

A Web Service Oriented Cloud Architecture for Maintaining Privacy and Auditability of Medical Reports

Amruta S.Dhange[1], Prof. R. V. Argiddi [2]

Department of Computer Science and Engineering, WIT Solapur, Maharashtra, India [1,2]

ABSTRACT: As Healthcare data is increasing day by day, security issues are raised. We can achieve this privacy using cloud in electronic health care system. So, we proposed to build privacy model in electronic healthcare systems with the help of the cloud. Cloud will be accessed to only authenticated users so we can say that privacy policy will be achieved. We proposed to implement some features like key management for file sharing and search pattern (patient records and treatment document), privacy-preserving data storage of patient records, and retrieval, especially for retrieval at emergencies, and auditability for preventing misuse of health data. Using key management we proposed to implement search pattern and file (patient or treatment records) sharing between patient and doctor as well as between patient and insurance user. The file can be accessed only when key is matched. Privacy preserving data storage will store the data in encrypted form using key. Retrieval for fetching patient or treatment records at emergency and auditability prevents misuse of health data by identifying leakage and leaker of the data.

KEYWORDS: key management, auditability, eHealth, leakage, privacy.

I. INTRODUCTION

As the Electronic healthcare (eHealth) systems have improving widely, people getting more advantages than the previous traditional paper-based systems. People dealing with their data with higher efficiency and better accuracy. The eHealth systems like mobile healthcare system enable patients to efficiently collect personal health data and obtain any medical services at emergencies. But patient records are more sensitive which contains all personal information of a particular person. This eHealth system can save life of people as it can be accessible to anywhere so that doctor can treat a patient at emergencies. As these systems are getting more popular, large amount of data of patients also adding to the system. According to government research more than 8 millions of data is leaked from last two years. No control is there on the patient's personal record. Therefore attackers are easily using the personal data of patients i.e. this data is easily accessible anywhere and anyone can access it or read it. To overcome such problem we have some schemes to make their data records as private and limited accessible. Some people among us may think that why to make the patient records secure? As we know the companies employer may not give a job to patient if he know about patient's disease. In the same way, insurance company will not provide any policy to that patient as he has some disease. It is not a good thing if that patient is not getting job or any insurance policies or any problems that may generated due to this leakage of data.

Therefore, we need a technique which makes the patients records more secure and give limited access.

In our project, we implemented a technique to make the healthcare data secure. We have focused on some features for making data auditable and more secure. The following diagram shows the system architecture. In our project we have 3 actors as patient, doctor and insurance company. These actors access and store the data through web application. These manipulated data will be stored in cloud. This is accessible to only authenticated user based on the attribution. The flow of project is as follows:

- The patient shares the file which contains information of his health to doctor and insurance user and he has an option to select doctor for treatment.

DOI: 10.15680/IJIRCCE.2019. 0702048

- Doctor accesses the file of patient and share treatment file accordingly. Both can access the file only when the attribute shared between them is matched.
- Insurance company can only view patient records.

1.1. System Architecture:

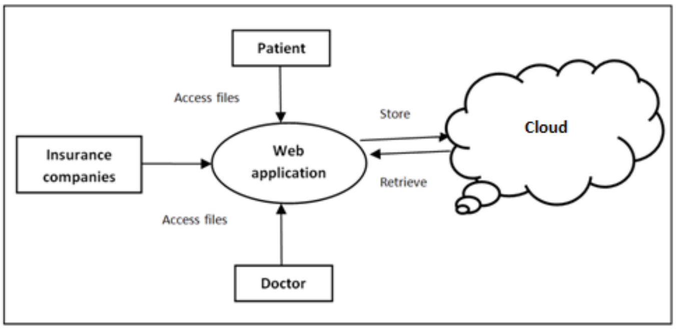


Fig1. System Architecture

1.2. List of Actors and role of actors in Healthcare system:

1.2.1. Admin:

In this project, we have an admin who controls overall system. Admin can create the patients accounts. Admin maintains the list of doctors with their specialization information and with some contact information so that patients can easily get in touch with doctors at any emergencies. Admin also maintains the list of insurance companies with their contact details.

1.2.2. Patient:

Patient will have to register to our site for accessing any treatments. Patients have following roles:

I. File uploading and sharing:

Patient will upload a report or health information file on the site and select the doctor for treatment. While uploading file patient will add file and attribute keywords (encryption key) which will be shared with authenticated doctors as well as insurance users.

II. Audit:

To prevent the misuse of the patient records, audit file is generated. Audit is to test integrity of data. Only patient have authority to access this audit file. Here RS value is calculated where S is the hash value and R is any random number and divide this value by N as constant integer number and find out the mod value and compare them. If the values are equal then we can say data is intact otherwise data is corrupted.

III. Search File:

For searching file, patient or doctor or insurance user should have a key which was generated at the time of file uploading. If key is matched then only one can find out the file.

1.2.3. Doctor:

Doctor can view the patient records by login to the system and give the treatment accordingly. Doctor also uploads and share file by using some file attribute (master key).

1.2.4. Insurance company:

Insurance users can access the patient record by authentication.

DOI: 10.15680/IJIRCCE.2019. 0702048

II. LITERATURE REVIEW

Linke Guo, Chi Zhang, Jinyuan Sun and Yuguang Fang have focused on “A Privacy-Preserving Attribute-Based Authentication System for Mobile Health Networks”. They have implemented a decentralized system which leverages some verifiable attributes to authenticate each other while preserving identity privacy. They also proposed to design authentication strategies for privacy. Finally, they have calculated the security and computational overheads for their schemes via some experiments.

Longhua Zhang, Gail-Joon Ahn and Bei-Tseng Chu have implemented “A Rule-Based Delegation Framework for Healthcare Information Systems”. They have introduced an approach to specify delegation methods for privacy of health care data. They have evaluated the feasibility of our framework through enforcement, policy specification and a proof-of-concept implementation on healthcare information.

Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang have proposed to work on healthcare information by implementing “An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks”. Vehicular Ad Hoc Networks (VANET) plays vital role in privacy preserving issues. If any attacks or misuse of the network happens then it will cause destructive consequences. Therefore all operations of the network performed well. They proposed a security system for VANETs to achieve privacy desired by vehicles and traceability for satisfying main security issues including authentication, integrity, and confidentiality.

M. ARUN KUMAR and Mr. B. BHARATH KUMAR have implemented “Privacy Preserving and Auditability Techniques for Cloud Assisted Mobile Access of Health Data”. They have implement a privacy system using key management for securing healthcare data. Retrieval and storage will be performed by securely by preserving privacy issues.

Pradeep Ray and J. Wimalasiri have focused on “The need for technical solutions for maintaining the privacy of EHR”. In this paper a model of “proof of retrieve ability”, where spot-checking as well as error-correcting codes have been used for ensuring both “possession” as well as data files “retrieve ability” on archive service systems. Though the existing systems strive for providing verification of integrity for various systems of data storage, the issue that involves supporting public auditability as well as data dynamics is not fully addressed.

Panagiotis Papadimitriou and Hector Garcia-Molina have implemented “Data Leakage Detection”. They have implemented a model which finds guilty agents who leaks the data and leakage of the data. They calculated the percentage of leakage of data by using data allocation strategies.

Wei-Bin Lee *and* Chien-Ding Lee have proposed “a cryptographic key management solution for HIPAA privacy-y or security regulations”. For providing security to healthcare privacy HIPAA regulations creates a principle to assure that patient’s records are more secure and set limits to use and disclosure. Key management solution is designed to provide interoperations in the Cryptographic mechanisms.

III. METHODOLOGY

3.1 Features Implemented for privacy preserving:

Key Management:

a) File uploading and File sharing

Patient and doctors upload or share files between each other. These files are shared with a private key. If key is matched then only one can access the file. The key is generated by using ABE (Attribute based encryption) algorithm. Simultaneously, the files are encrypted using AES (Advanced Encryption Standard) algorithm.
Patient also share files to authorized insurance user. These files are shared using IBE (Identity-based Encryption).
Identity-based Encryption systems allow patient to generate a public key from a known identity value.

A trusted party, called the Private Key Generator (PKG), generates the corresponding private keys. To operate, the PKG first publishes a master public key, and retains the corresponding master private key (referred to as master key). Given the master public key, patient can compute a public key corresponding to the identity by combining the master public key with the identity value. To obtain a corresponding private key, the patient authorized to use the identity ID contacts the PKG, which uses the master private key to generate the private key for identity ID.
As a result, IBE makes it possible for patient to encrypt message with no prior distribution of keys to insurance users.

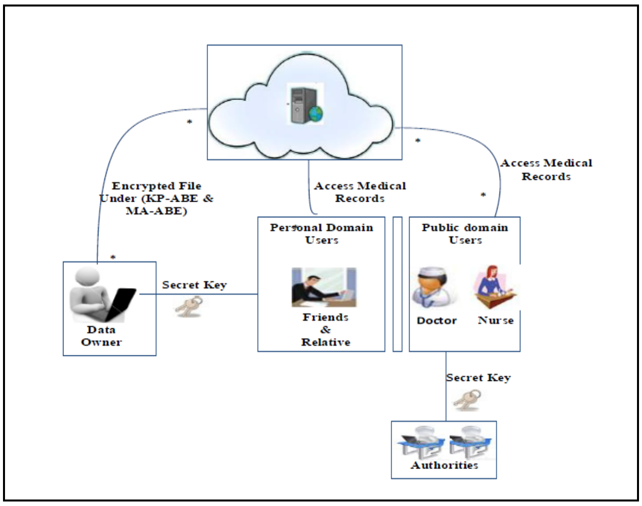


Fig 3. Architecture of Medical records sharing

b) Treatment

Doctor gives treatment to patient and share some files to patients. These files are encrypted using AES algorithm. These files are accessed and uploaded using a master key.

3.2 File Searching

Patient, doctor or insurance users search the files which are shared or uploaded by using keyword which was shared during file uploading. Searchable Symmetric Encryption (SSE) encrypts keyword. If keyword is matched then only one can find the file.

3.3 Auditability:

1. Leakage detection

All actors in this project have authority to detect the leakage of their data using watermarking.
To prevent the misuse of the treatment records, 4 realistic objects (marker) are added at the end of file as well as we adds username who will download the file after marker (as watermarking text).By using these marker everyone can detect the leakage and leaker of the data.

2. Audit

Audit is to test integrity of data. Only patient have authority to access this audit file. Patient checks and find out corrupted data by using 3 steps. We used Zero-Knowledge Protocol (ZKP) algorithm to audit file. To find corrupted data, we first need three variables called S,R, and N where S is the value which is calculated by using SHA algorithm ,R is random number and N is constant value.

The steps are as follows:
Step 1: Challenge
Auditor:
Here S is the hash value and R is any random number which is generated by auditor and N as constant integer number. It has S^2%N. It generates R as a random number and sends it to cloud.

Step 2: Request:
Cloud
Here RS value is calculated where S is the hash value and R is any random number which is taken from auditor and divide this value by N as constant integer number and find out the mod value

Step 3: Verification:
Auditor

Calculate

1. **((RS % N)^2)%N**
2. **((Rˆ2 % N) * (Sˆ2 % N))%N**

And compare the above 2 formulas as follows:

((Rˆ2 % N) * (Sˆ2 % N))%N== ((RS % N) ^2) %N

If the values are equal then we can say data is intact otherwise data is corrupted.

3.4 Algorithm:
First patient select the file, he wants to share to doctor. Then patient must enter correct attribute which it should be matched with that doctors attribute, to which he want to share. Using that attribute we generate key using ABE algorithm and using that key we encrypt the file using AES algorithm.

Doctor can give the treatment to patient by sending treatment file, which is encrypted by AES algorithm.
Patient also shares his report to Insurance user using IBE algorithm.

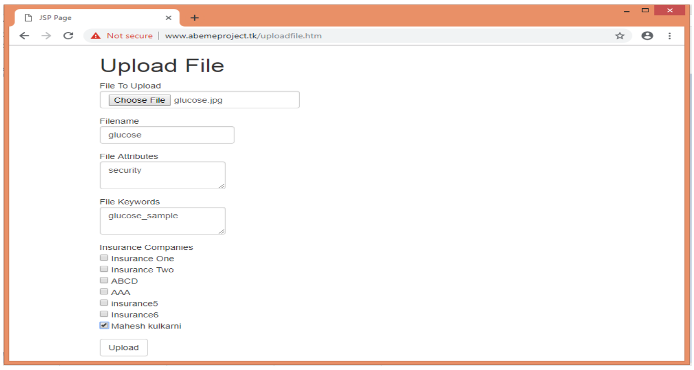
Patient, Doctor and Insurance users search the files using keyword which was shared during file uploading by patient and that keyword is encrypted by SSE encryption.

Patient audit his file by applying modified ZKP algorithm.

All actors detect the leakage of their data using content watermarking technique.

IV. EXPERIMENTAL RESULT

System provides privacy and security for medical reports or health information file while patient uploading and sharing it to Doctor and Insurance User by using ABE,AES and IBE respectively.
The following fig illustrates file uploading and sharing by patient to Doctor or Insurance User or both.



Upload File

File To Upload
Choose File glucose.jpg

Filename
glucose

File Attributes
security

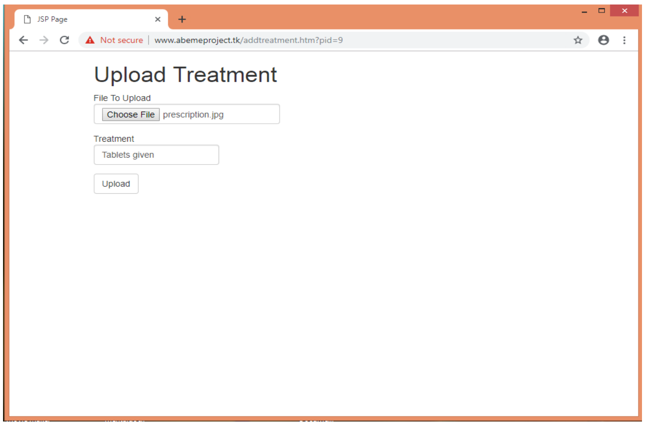
File Keywords
glucose_sample

Insurance Companies
□ Insurance One
□ Insurance Two
□ ABCD
□ AAA
□ insurance5
□ Insurance6
☑ Mahesh kulkarni

Upload

Figure 1. File uploading and sharing by patient

The following figure illustrates doctor will upload and share the file for giving treatment to the patient.



Upload Treatment

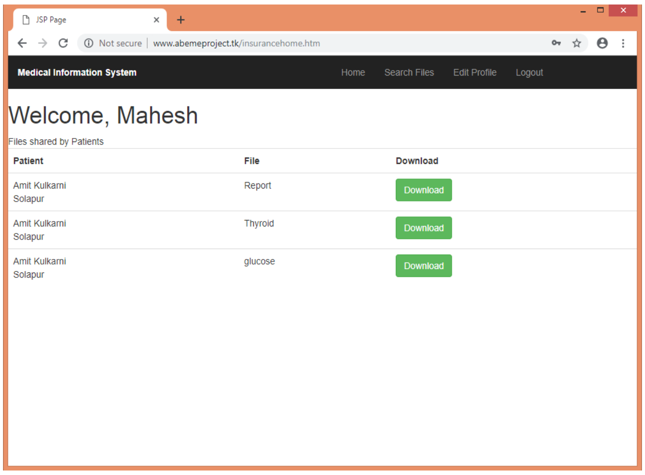
File To Upload
Choose File prescription.jpg

Treatment
Tablets given

Upload

Figure 2. File uploading and sharing by doctor (Tratment file)

The following figure shows patient’s records which is shared by patient to insurance user.


JSP Page
Not secure | www.abemeproject.tk/insurancehome.htm
Medical Information System
Home
Search Files
Edit Profile
Logout

Welcome, Mahesh

Files shared by Patients

Patient	File	Download
Amit Kulkarni Solapur	Report	Download
Amit Kulkarni Solapur	Thyroid	Download
Amit Kulkarni Solapur	glucose	Download

Figure 3. Patient details with shared file (Insurance User panel)

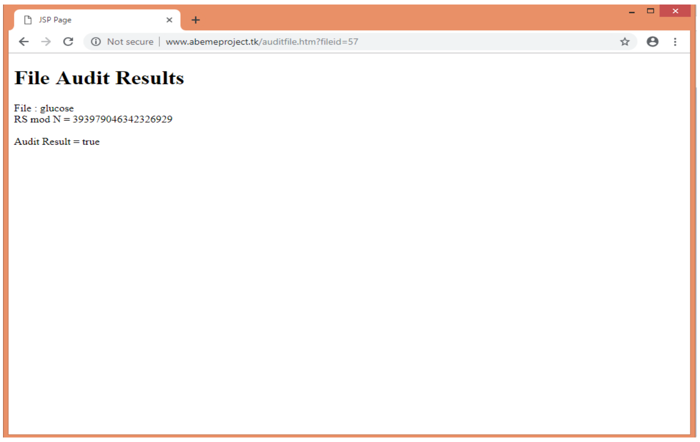
DOI: 10.15680/IJIRCCE.2019. 0702048

Audit is to test integrity of data.Patients have the authority to access the audit file.He checks and find out corrupted data by using ZKP algorithm.By using following formula auditor (Patient) checks his file.

$$((R\hat{}2 \ \% \ N) * (S\hat{}2 \ \% \ N))\%N == ((RS \ \% \ N) \ \hat{}2) \ \%N$$

If the values are equal then we can say data is intact (i.e Audit Result=true) otherwise data is corrupted (i.e Audit Result= false).

The following figure shows result of audited file.



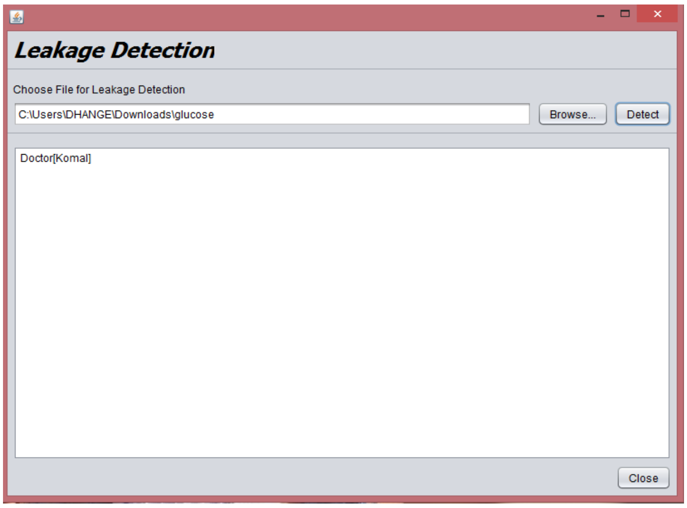
File Audit Results

File : glucose
RS mod N = 393979046342326929

Audit Result = true

Figure 4. Audit Result

All actors of the proposed sytem detects the leakage of their data and identify possible source(s) of leakage (i.e.,the authorized party that did it).
The following fig shows detection of data leakage and leaker name.



Leakage Detection

Choose File for Leakage Detection

C:\Users\DHANGE\Downloads\glucose

Doctor[Komal]

Figure 5.Leakage Detection

V. CONCLUSION

In this paper, we have built privacy into eHealthcare system with the help of cloud. eHealth systems helps to save life of people by treating patients at emergencies. To make data secure, we have implemented some features like key management for sharing, searching and access patterns of patient and doctors data. We also implemented auditability to prevent the data corruption. We also provided authentication system to prevent misbehavior of the data. And we used SHA algorithm for implementing auditability. We used ABE, AES and IBE algorithms for implementing key management system. We encrypt the healthcare data which is distributed between the patient and doctor as well as between patient and insurance user. We also detect whether patient's health data have been illegally distributed, and identify possible source(s) of leakage. The above features implement successfully for preserving the privacy of data.

REFERENCES

1. *Yue Tong, Jinyuan Sun, Sherman S. M. Chow, and Pan Li, "Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability"*, IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, VOL. 18, NO. 2, MARCH 2014
2. *Wei-Bin Lee and Chien-Ding Lee have proposed "a cryptographic key management solution for HIPAA privacy-y or security regulations"*, IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE, VOL. 12, NO. 1, JANUARY 2008
3. *A*lberto Trombetta, Wei Jiang and Lorenzo Bossi- "Privacy-Preserving Updates to Anonymous and Confidential Databases" *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 4, JULY/AUGUST 2011*
4. *Linke Guo, Chi Zhang, Jinyuan Sun and Yuguang Fang have focused on "A Privacy-Preserving Attribute-Based Authentication System for Mobile Health Networks*", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 9, SEPTEMBER 2014
5. *Longhua Zhang, Gail-Joon Ahn and Bei-Tseng Chu have implemented "A Rule-Based Delegation Framework for Healthcare Information Systems"*, University of North Carolina at Charlotte, ACM Transactions on Information and System Security, Vol. 6, No. 3, August 2003
6. *Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang have proposed to work on healthcare information by implementing "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks"*, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 21, NO. 9, SEPTEMBER 2010
7. *M. ARUN KUMAR and Mr. B. BHARATH KUMAR have implemented "Privacy Preserving and Auditability Techniques for Cloud Assisted Mobile Access of Health Data"*, Volume 3, Issue 1 JULY 2015, IJOEET
8. *P. RayandJ. And Wimalasiri have focused on "The need for technical solutions for maintaining the privacy of HER"*. In Proc. IEEE, 28th Annual International Conf., New York City, NY, USA, Sep. 2006, pp. 4686–4689
9. *Panagiotis Papadimitriou, Hector Garcia-Molina, "Data Leakage Detection"* , IEEE transactions on knowledge and data engineering, vol. 23, no. 1, January 2011
10. *R. Agrawal and J. Kiernan, "Watermarking Relational Databases,"* Proc. 28th Int'l Conf. Very Large Data Bases (VLDB '02), VLDB Endowment, pp. 155-166, 2002.
11. *B. Mungamuru and H. Garcia-Molina, "Privacy, Preservation and Performance"*: The 3 P's of Distributed Data Management," technical report, Stanford Univ., 2008.
12. *V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attributed-based encryp- tionforfine-grained access control of encrypted data,"* inProc. ACMConf. Comput. Commun. Security, 2006, pp. 89–98.
13. *Pradeep Ray and Jaminda Wimalasiri, "The need for technical solutions for maintaining the privacy of EHR"*, 2006 International Conference of the IEEE Engineering in Medicine and Biology Society.